## **CLAIMS**

What is claimed is:

		· ·
	15uk	1. A method for caching secure network communications in a computer
	2 /	network, comprising placing at least one secure reverse proxy among at least one
	3	web server and at least one web browser, wherein the at least one secure reverse
72.	4	proxy caches secure content.
A Null And		
We that that that the	1	2. A method for secure network communications, comprising:
Hart them	2	coupling at least one network appliance among at least one web server and a
	3	least one web browser;
the that that that their that	4	establishing a secure session between the at least one network appliance and
	5	the at least one web browser, wherein the at least one web browser sends an
≓ ` .≛	6	encrypted request for content using a secure session protocol;
	7	decrypting the encrypted request for content at the at least one network
	8	appliance;
	9	examining at least one network appliance's local cache to locate the content;
	10	encrypting the content from the at the at least one network appliance's local
	11	cache using an established secure protocol; and
	12	sending the content to the at least one web browser, wherein reducing the
	13	number of requests at the web server for establishing a secure network connection
	14	improves network efficiency.

1	3. The r	nethod of claim 2, wherein the local cache includes non-volatile
2	memory.	
1	4. The 1	nethod of claim 2, wherein the at least one network appliance
2	and the at least one	Web server are collocated.
1	5. The r	nethod of claim 2, wherein the content includes an HTTP page.
1	6. The r	nethod of claim 2, wherein decrypting further includes:
2	determining	the content requested by the at least one web browser is not
3	present in the at leas	t one network appliance's local cache;
4	forwarding t	he request for content to the at least one web server using a
5	separate secure sess	on;
5	receiving ba	k from the at least one web server to the at least one network
) • 7	appliance a response	containing the requested content, wherein communication
8	between the at least	one network appliance and the at least one web server is secure;
9	and	
10	caching the	equested content locally at the network appliance for future
11	requests.	
1	7. The 1	nethod of claim 2, wherein the secure session uses Transport
2		

session with the at least one web server;  establishing a first secure session using a first secure session protocol  between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an encrypted request for a HTTP page;  decrypting the encrypted request for a HTTP page at the at least one SRP		1	8. The method of claim 2, wherein the secure session uses secure
Protocol Secure ("IPSec") techniques.  1 10. A method for caching secure network communications, comprising: coupling at least one Secure Reverse Proxy ("SRP") among at least one web server and at least on web browser wherein the at least one SRP intercepts requests from the at least one web browser to establish a secure network communication session with the at least one web server; establishing a first secure session using a first secure session protocol between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an encrypted request for a HTTP page; decrypting the encrypted request for a HTTP page at the at least one SRP using the first secure session protocol, wherein the at least one SRP examines a loca cache determining if the HTTP page is available; retrieving the HTTP page if available from the local cache using the first secure session protocol; sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session; establishing a second secure session using a second secure session protocol		2	Socket Layer protocol.
1 10. A method for caching secure network communications, comprising: 2 coupling at least one Secure Reverse Proxy ("SRP") among at least one web 3 server and at least on web browser wherein the at least one SRP intercepts requests 4 from the at least one web browser to establish a secure network communication 5 session with the at least one web server; 6 establishing a first secure session using a first secure session protocol 7 between the at least one SRP and the at least one web browser, wherein the at least 8 one web browser sends an encrypted request for a HTTP page; 9 decrypting the encrypted request for a HTTP page at the at least one SRP 10 using the first secure session protocol, wherein the at least one SRP examines a local 11 cache determining if the HTTP page is available; 12 retrieving the HTTP page if available from the local cache using the first secure session protocol; 13 sending the encrypted HTTP page to the at least one web browser if the 14 HTTP page is available from the local cache using the first secure session; 15 establishing a second secure session using a second secure session protocol		1	9. The method of claim 2, wherein the secure session uses Internet
coupling at least one Secure Reverse Proxy ("SRP") among at least one web server and at least on web browser wherein the at least one SRP intercepts requests from the at least one web browser to establish a secure network communication session with the at least one web server; establishing a first secure session using a first secure session protocol between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an encrypted request for a HTTP page; decrypting the encrypted request for a HTTP page at the at least one SRP using the first secure session protocol, wherein the at least one SRP examines a loca cache determining if the HTTP page is available; retrieving the HTTP page if available from the local cache using the first secure session protocol; sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session protocol; sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session; establishing a second secure session using a second secure session protocol		2	Protocol Secure ("IPSec") techniques.
server and at least on web browser wherein the at least one SRP intercepts requests from the at least one web browser to establish a secure network communication session with the at least one web server; establishing a first secure session using a first secure session protocol between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an encrypted request for a HTTP page; decrypting the encrypted request for a HTTP page at the at least one SRP using the first secure session protocol, wherein the at least one SRP examines a local cache determining if the HTTP page is available; retrieving the HTTP page if available from the local cache using the first secure session protocol; sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session; establishing a second secure session using a second secure session protocol		1 .	10. A method for caching secure network communications, comprising:
session with the at least one web server;  establishing a first secure session using a first secure session protocol  between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an encrypted request for a HTTP page;  decrypting the encrypted request for a HTTP page at the at least one SRP using the first secure session protocol, wherein the at least one SRP examines a local cache determining if the HTTP page is available;  retrieving the HTTP page if available from the local cache using the first secure session protocol;  sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session;  establishing a second secure session using a second secure session protocol	of the party	2	coupling at least one Secure Reverse Proxy ("SRP") among at least one web.
session with the at least one web server;  establishing a first secure session using a first secure session protocol  between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an encrypted request for a HTTP page;  decrypting the encrypted request for a HTTP page at the at least one SRP using the first secure session protocol, wherein the at least one SRP examines a local cache determining if the HTTP page is available;  retrieving the HTTP page if available from the local cache using the first secure session protocol;  sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session;  establishing a second secure session using a second secure session protocol		3	server and at least on web browser wherein the at least one SRP intercepts requests
session with the at least one web server;  establishing a first secure session using a first secure session protocol  between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an encrypted request for a HTTP page;  decrypting the encrypted request for a HTTP page at the at least one SRP using the first secure session protocol, wherein the at least one SRP examines a local cache determining if the HTTP page is available;  retrieving the HTTP page if available from the local cache using the first secure session protocol;  sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session;  establishing a second secure session using a second secure session protocol	# # #	4	from the at least one web browser to establish a secure network communication
between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an encrypted request for a HTTP page;  decrypting the encrypted request for a HTTP page at the at least one SRP using the first secure session protocol, wherein the at least one SRP examines a local cache determining if the HTTP page is available;  retrieving the HTTP page if available from the local cache using the first secure session protocol;  sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session;  establishing a second secure session using a second secure session protocol	must stam	5	session with the at least one web server;
using the first secure session protocol, wherein the at least one SRP examines a local cache determining if the HTTP page is available;  retrieving the HTTP page if available from the local cache;  encrypting the HTTP page retrieved from the local cache using the first secure session protocol;  sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session;  establishing a second secure session using a second secure session protocol		6	establishing a first secure session using a first secure session protocol
using the first secure session protocol, wherein the at least one SRP examines a local cache determining if the HTTP page is available;  retrieving the HTTP page if available from the local cache;  encrypting the HTTP page retrieved from the local cache using the first secure session protocol;  sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session;  establishing a second secure session using a second secure session protocol	f elim thut	7	between the at least one SRP and the at least one web browser, wherein the at least
using the first secure session protocol, wherein the at least one SRP examines a local cache determining if the HTTP page is available;  retrieving the HTTP page if available from the local cache;  encrypting the HTTP page retrieved from the local cache using the first secure session protocol;  sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session;  establishing a second secure session using a second secure session protocol		8	one web browser sends an encrypted request for a HTTP page;
cache determining if the HTTP page is available; retrieving the HTTP page if available from the local cache; encrypting the HTTP page retrieved from the local cache using the first secure session protocol; sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session; establishing a second secure session using a second secure session protocol	af <u>Sa</u>	9	decrypting the encrypted request for a HTTP page at the at least one SRP
retrieving the HTTP page if available from the local cache; encrypting the HTTP page retrieved from the local cache using the first secure session protocol; sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session; establishing a second secure session using a second secure session protocol		10	using the first secure session protocol, wherein the at least one SRP examines a local
encrypting the HTTP page retrieved from the local cache using the first secure session protocol; sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session; establishing a second secure session using a second secure session protocol		11	cache determining if the HTTP page is available;
secure session protocol; sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session; establishing a second secure session using a second secure session protocol		12	retrieving the HTTP page if available from the local cache;
sending the encrypted HTTP page to the at least one web browser if the  HTTP page is available from the local cache using the first secure session;  establishing a second secure session using a second secure session protocol		13	encrypting the HTTP page retrieved from the local cache using the first
HTTP page is available from the local cache using the first secure session; establishing a second secure session using a second secure session protocol		14	secure session protocol;
establishing a second secure session using a second secure session protocol		15	sending the encrypted HTTP page to the at least one web browser if the
		16	HTTP page is available from the local cache using the first secure session;
with the at least on web server if the HTTP page is not available from the local		17	establishing a second secure session using a second secure session protocol
		18	with the at least on web server if the HTTP page is not available from the local

15	Cache,	wherein the second secure session is maintained,
20	)	encrypting the request for a HTTP page using the second secure session
21	protoc	ol;
22	2	forwarding the request for a HTTP page encrypted using the second secure
23	session	n to the at least one web server:
24	1	receiving from the at least one web server an encrypted HTTP page using the
25	second	I secure session;
26	5	decrypting the encrypted HTTP page using the second secure session
五 五 五	7 protoc	ol;
<b>三</b> 28	3	storing the HTTP page in the at least one SRP's local cache;
以 订 29	)	encrypting the HTTP page using the first secure session protocol; and
30	)	sending the HTTP page to the at least one web browser using the first secure
	l session	1.
	l	11. The method of claim 10, wherein coupling includes connecting the
2	SRP a	nd web server using a dedicated line.
1	1	12. The method of claim 10, wherein coupling includes having the web
2	2 server	and SRP collocated.
1	1	13. The method of claim 10, wherein storing includes using non-volatile
2	2 media	to store the content.
3	3	14. The method of claim 10, wherein storing includes encrypting the
4	4 conten	t using a third secure session protocol.
	C:\NrPo	rtbl\PALIB1\PBM\1327324_5.DOC 15

1	15. The method of claim 10, wherein the first secure session protocol
2	includes Transport Layer Security protocol.
1	16. The method of claim 10, wherein the second secure session protocol
2	includes Transport Layer Security protocol.
1	17. The method of claim 10, wherein the third secure session protocol
2	includes Transport Layer Security protocol
1	18. The method of claim 10, wherein the first secure session protocol
2	includes Secure Socket Layer protocol.
1	19. The method of claim 10, wherein the second secure session protocol
2	includes Secure Socket Layer protocol.
1	20. The method of claim 10, wherein the third secure session protocol
2	includes Secure Socket Layer protocol
1	21. The method of claim 10, wherein the first secure session protocol
2	includes Internet Protocol Secure ("IPSec") techniques.
1	22. The method of claim 10, wherein the second secure session protocol
2	includes Internet Protocol Secure ("IPSec") techniques.
	C:\NrPortb\\PALIB1\PBM\1327324_5.DOC 16

Ö
inter inter
Ū
<b>5</b>
``\
•
Ü
1
1
1

		i de la companya de
	1	23. The method of claim 10, wherein the third secure session protocol
	2	includes Internet Protocol Secure ("IPSec") techniques.
	1	24. A method for caching secure content in a Secure Reverse Proxy
	2	("SRP") in an secure network, comprising:
	3	coupling at least one SRP among at least one web browser and at least one
1 1 1	4	web server wherein the at least one SRP receives from the at least one web browser
that mad don the that that that that	5	requests for establishing a first secure session;
	6	establishing the first secure session using a first secure session protocol
	7	between the at least one SRP and the at least on web browser, wherein the web
, 4m.Q	8	browser sends an encrypted request for content to the at least one SRP;
	9	decrypting the encrypted request for content from the at least one web
to that that that dies it all	10	browser at the at least one SRP using the first secure session protocol, wherein the at
	11	least one SRP determines that the at least one SRP does not possess the requested
	12	content;
	13	establishing a second secure session using a second secure session protocol
	14	between the at least one SRP and the at least one web server, wherein the second
	15	secure session is maintained;
	16	encrypting the request for content from the at least one web browser using
	17	the second secure session protocol;
	18	sending the encrypted request for content to the at least one web server using
	19	the second secure session;
	20	receiving the content from the at least on web server at the least one SRP
		C:\NrPorth\\PALIBI\\PBM\\1327324_5 DOC 17

2	21	using the second secure session;
2	22	decrypting the content using the second secure session protocol;
2	23	storing the requested content locally in a memory at the at least one SRP; and
2	24	retrieving the content from the memory at the at least one SRP upon
2	25	subsequent requests for the content.
		~1
	1	25. The method of claim 24, wherein storing includes encrypting the
1	2	content using a third secure session protocol, wherein the third secure session
and there there had	3	protocol is known only to the at least one SRP.
1) 1)		
the made	1	26. The method of claim 24, wherein storing includes using non-volatile
4 cent	2	media.
***************************************		
	1	27. The method of claim 24, wherein coupling includes establishing a
	2	dedicated secure line between the SRP and the web server.
	1	28. The method of claim 24, wherein coupling includes collocating the
	2	web server and the SRP.
	1	29. The method of claim 24, wherein content includes an HTTP page.
	1	30. The method of claim 24, wherein the first secure session includes
	2	Transport Layer Security protocol.

1	31. The method of claim 24, wherein the second secure session includes
2	Transport Layer Security protocol.
1	32. The method of claim 24, wherein the first secure session includes
2	Secure Socket Layer protocol.
1	33. The method of claim 24, wherein the second secure session includes
2	Secure Socket Layer protocol.
1	34. The method of claim 24, wherein the first secure session includes
2	Internet Protocol Secure ("IPSec") techniques.
1	35. The method of claim 24, wherein the second secure session includes
2	Internet Protocol Secure ("IPSec") techniques.
1	36. The method of claim 24, wherein storing includes encrypting the
2	requested HTTP page.
1	37. A system for caching secure communications in a network
2	comprising:
3	at least one web server;
4	at least one web browser;
5	at least one Secure Reverse Proxy ("SRP") coupled among the at least one

6	web server and the at least one web browser, wherein the at least one SRP caches
7	secure content.
1	38. The system of claim 37, wherein the at least one web browser, the at
2	least one web server, and at least one SRP use Transport Layer Security protocol to
3	establish a secure session.
1	39. The system of claim 37, wherein the at least one web browser, the at
2	least one web server, and at least one SRP use Secure Socket Layer protocol to
3	establish a secure session.
1	40. The system of claim 37, wherein the at least one web browser, the at
2	least one web server, and at least one SRP use Internet Protocol Secure ("IPSec")
3	techniques to establish a secure session.
1	41. A method for secure communications in a network, comprising:
2	caching responses including secure content from at least one web server to at
3	least one web browser in at least one Secure Reverse Proxy ("SRP"), wherein the at
4	least one SRP is coupled among the at least one web server and the at least one web
5	browser; and
6	enabling future requests for the same secure content to be processed by the at
7	least one SRP.

1	42. A system for emancing secure communications in a computer
2	network, comprising:
3	at least one Secure Reverse Proxy ("SRP") coupled among at least one web
4	server and at least one browser, wherein the at least one SRP establishes a secure
5	session between the at least one SRP and the at least one web browser;
6	the at least one web browser sending to the at least one SRP an HTTP page
7	request encrypted using the secure session protocol;
8	the at least one SRP decrypting the HTTP page request, wherein the SRP
9	examines a local cache to locate the HTTP page, retrieves the HTTP page, encrypts
10	the HTTP page from the local cache using the established secure session protocol,
11	and sends the HTTP page to the at least one web browser using the secure session
12	reducing the messages sent to the web server improving the efficiency of the
13	network.
1	43. The system of claim 42, wherein the secure session is established
2	using Transport Layer Security protocol.
1	44. The system of claim 42, wherein the secure session is established
2	using Secure Socket Layer protocol.
1.	45. The system of claim 42, wherein the secure session is established
2	using Internet Protocol Secure ("IPSec") techniques.

1	46. The system of claim 42, further comprising:
2	the at least one \$RP establishing a separate secure session with the at least
3	one web server, wherein the at least on web server forwards the HTTP page request
4	to the at least one web server using a separate secure session;
5	the at least one web server sending to the at least one SRP a response
6	containing the requested HTTP page, wherein communication between the at least
7	one SRP and the at least one web server is secure using the separate secure session;
8	and
9	the at least one SRP caching the requested HTTP page for future requests.
1	47. A computer readable medium, comprising executable instructions for
2	caching secure content in computer network which, when executed in a processing
3	system, causes the system to:
4	couple at least one Secure Reverse Proxy ("SRP") among at least one web
5	server and at least one browser;
6	direct requests for establishing a secure connection from the at least one web
7	browser to the at least one SRP, wherein the SRP responds by initiating an initial
8	secure handshake;
9	establish a secure session between the at least one SRP and the at least one
10	web browser, wherein the at least one web browser sends an HTTP page request
11	encrypted using a secure session protocol;
12	decrypt the HTTP page request at the at least one SRP, wherein the SRP
13	examines a local cache to locate the HTTP page;
14	retrieve the HTTP page from the local cache;
	1

1	.5	encrypt the HTTP page from the local cache at the at least one SRP using the
1	6	established secure protocol; and
1	7	send the HTTP page to the at least one web browser, wherein contact with
1	8	the at least one web server is reduced improving the effective efficiency of the
1	9	network.
	1	48. The computer readable medium of claim 47, further comprising
*****	2	instructions that when executed in a processing system cause the system to:
r The strain	3	forward the HTTP page request to the at least one web server using a
	4	separate secure session when the HTTP page is not present in the local cache;
	5	receive from the at least one web server to the at least one SRP a response
	6	containing the requested HTTP page wherein communication between the at least
e to the total and an	7	one SRP and the at least one web server is secure using a separate secure session;
	8	and
*\$	9	cache the requested HITP page locally at the SRP for future requests.
	1	49. An electromagnetic medium containing executable instructions for
	2	improving secure connections in computer network communications which, when
	3	executed in a processing system, causes the system to:
	4	couple at least one Secure Reverse Proxy ("SRP") among at least one web
	5	server and at least one browser;
	6	direct requests for establishing a secure connection from the at least one web
	7	browser to the at least one SRP, wherein the SRP responds by initiating an initial
	8	secure handshake;
		4.5

9	establish a secure session between the at least one SRP and the at least one
10	web browser, wherein the at least one web browser sends an HTTP page request
11	encrypted using a secure session protocol;
12	decrypt the HTTP page request at the at least one SRP, wherein the SRP
13	examines a local cache to locate the HTTP page;
14	retrieve the HTTP page from the local cache;
15	encrypt the HTTP page from the local cache at the at least one SRP using the
□16	established secure protocol; and
17 17 18 19	send the HTTP page to the at least one web browser, wherein contact with
18	the at least one web server is reduced improving the effective efficiency of the
<u>J</u>	network.
	50. The electromagnetic medium of claim 49, further comprising
2	instruction that when executed in a processing system cause the processing system
. 3	to:
4	forward the HTTP page request to the at least one web server using a
5	separate secure session when the HTTP page is not present in the local cache;
6	receive from the at least one web server to the at least one SRP a response
7	containing the requested HTTP page wherein communication between the at least
8	one SRP and the at least one web server is secure using a separate secure session;
9	and
10	cache the requested HTTP page locally at the SRP for future requests.
	ackslash